UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------x
UNITED STATES OF AMERICA,

Plaintiff,

-against-

MEMORANDUM AND ORDER
20-cv-0473 (EK) (RLM)

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a/ Tollfreedeals.com and SIP RETAIL d/b/a sipretail.com,

Defendants.
----------x

ERIC KOMITEE, United States District Judge:

Defendants Nicholas and Natasha Palumbo are residents of Arizona. Together, they manage the defendant companies Ecommerce National (doing business as "TollFreeDeals") and SIP Retail. Those companies serve as "intermediary carriers" in the telecommunications industry, introducing hundreds of millions of "robocalls" into the United States. The government alleges that the Defendants are key participants in a large, ongoing telecommunications fraud, and seeks a preliminary injunction under 18 U.S.C. § 1345 to enjoin their fraudulent conduct. For the reasons set forth below, the government's application is GRANTED.

Background

Defendants operate telecommunications carriers that connect calls placed over the internet, known as voice-over-internet

protocol ("VoIP") calls, to phone lines in the United States. *See* Dkt. No. 36, First Dalrymple Decl. ¶ 8(f). The call flow crossing Defendants' network typically originates abroad and routes through multiple intermediary carriers before reaching the recipients. *See* Dkt. No. 38, First Palumbo Decl. ¶¶ 14, 17; Dkt. No. 1-3, First Ralston Decl. ¶ 26. Defendants do business with other intermediaries, including foreign carriers, and specialize in short-duration and call-center traffic. *See* First Palumbo Decl. ¶ 10; First Ralston Decl. ¶¶ 26, 35. Defendants also sell U.S. phone numbers to their clients, which robocall recipients in the United States can use to call back foreign callers. *See* First Dalrymple Decl. ¶ 14; First Ralston Decl. ¶¶ 48-49; Dkt. No. 34-1, First Gerber Decl. ¶¶ 18-20.

The government alleges that Defendants have participated, and continue to participate, in fraudulent robocalling schemes involving the transmission of millions of calls to recipients in the United States. *See* Dkt. No. 1, Compl. ¶ 2. Various messages on these calls purport to come from government personnel such as "hearing administrators" and other officials at the Social Security Administration ("SSA");[1] from Deputy U.S. Marshals;[2] from police officers;[3] and from other officials.

[1] *See, e.g.*, First Gerber Decl. ¶ 12; Dkt. No. 49, Frankel Decl. ¶ 9; Dkt. No. 1-2, Bracken Decl. ¶¶ 6, 10, 13.
[2] *See* Bracken Decl. ¶ 6.
[3] *See id.* ¶¶ 8, 11.

Sometimes the numbers are spoofed to look like the numbers of government agencies. *See* First Ralston Decl. ¶¶ 39-40; Dkt. No. 1-2, Bracken Decl. ¶ 9. The messages typically inform the recipient that they have some problem vis-à-vis the government: for example, that their social security number has been compromised, Bracken Decl. ¶ 6; that a warrant has been issued for their arrest, *id.*; that they are subject to various tax and legal liabilities, First Ralston Decl. ¶ 11(b); or that they face imminent deportation, *id.* ¶ 11(c). The government also alleges that Defendants transmit robocalls from fraudsters who imitate tech support from well-known companies, like Apple and Microsoft, and from imposter loan officers, who offer pre-approved loans in return for an up-front fee. First Ralston Decl. ¶ 11(d), (e).

As discussed in more detail below, multiple recipients of these calls apparently believed the recorded messages, because they used the contact instructions provided to interact with live fraudsters who were able to deprive them of substantial sums. *See* Bracken Decl. ¶¶ 6-13 (laying out evidence from specific victims). Third parties regularly apprised the Defendants of the fraudulent call traffic traversing their system. *See, e.g.*, Dkt. No. 8, Second Ralston Decl. ¶¶ 4, 5. In these cases, the Defendants undertook only limited steps in response to these complaints. Specifically, they would block

the particular phone number (but not the entity) from which the reported call traffic emanated. *See, e.g.*, First Palumbo Decl. ¶¶ 35-36. Defendants' only other response was to pass along the complaint to the entity prior to them in the chain of call traffic. *See, e.g., id.*

Procedural History

The government filed suit on January 28, 2020. Together with its Complaint, the government applied for a Temporary Restraining Order ("TRO") pursuant to 18 U.S.C. § 1345. The proposed TRO would have required the Defendants to cease carrying any VoIP calls terminating in the United States and to cease selling U.S. call-back numbers, among other things. *See* Dkt. No. 3.

On the basis of the declarations attached to the Complaint and supplemental submissions,[4] the Court found probable cause to believe that Defendants were engaged in wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349. Wary, however, of awarding the broader relief sought without affording Defendants the opportunity to be heard, I directed that the Complaint be served on the Defendants and subsequently ordered the entry of a more limited TRO, with the consent of both parties. *See* Dkt. No. 18. This Order

[4] *See* First Ralston Decl.; Second Ralston Decl.; Bracken Decl.; Dkt. No. 7-3, Ashlea Bowens Decl.

prohibited Defendants from continuing to carry calls for, or provide call-back numbers to, sixteen specified companies and individuals who were, according to the government's evidence, associated with fraudulent call traffic on the Defendants' network. *See id.* The TRO went on to require (again, with Defendants' consent) the Defendants to terminate contracts with any other company or individual that was subsequently flagged as the source of fraudulent calls by a telecommunications organization or regulatory agency. *See id.*

Within weeks of the TRO's entry, evidence surfaced that one of Defendants' largest clients, Yodel Technology Services, LLC ("Yodel"), had sent multiple fraudulent calls through Defendants' system in connection with Internal Revenue Service ("IRS") imposter scams. Dkt. No. 31-1. Yodel was not one of the sixteen specified companies in the TRO, but under the TRO's agreed-upon terms, this development required Defendants to terminate their contract with Yodel. Defendants applied for relief from this requirement on the ground that severing ties with Yodel would essentially "shut down defendants' operations." Dkt. No. 31. In an effort (once again) to avoid potentially permanent harm to the Defendants' businesses before they had an opportunity to appear, I granted the relief Defendants sought. Dkt. No. 33.

Since then, the government has pressed the argument that the terms of the Court's TRO have been insufficient to put a stop to the ongoing fraud. On March 2, the government renewed its motion for the broader injunctive relief it initially sought, but this time in the form of a preliminary injunction. The preliminary injunction they now seek would (like the initial TRO request) prohibit Defendants from providing any call-termination services or carrying any VoIP calls in the United States, or providing tell-free telephone services for calls originating in the United States, among other things. *See* Dkt. No. 47-1, Proposed Preliminary Injunction Order.

In support of its contention, the government put forward substantial *additional* evidence of fraudulent traffic traversing the Defendants' telecommunications network, including specifically with respect to Yodel. *See e.g.*, First Gerber Decl. ¶¶ 8-22. The Court held oral argument on the preliminary injunction motion on March 3, 2020. At argument, the Court called for additional briefing on certain legal and factual issues from the parties; the parties both filed additional submissions on March 6, 2020.[5] *See* Dkt. Nos. 57-59.

Based on the totality of the evidence, I now conclude there is no narrower avenue reasonably available to enjoin the

[5] In total, the parties filed seventeen declarations.

fraudulent call traffic on Defendants' network and grant the preliminary injunctive relief sought by the government, for the reasons set forth below.

Legal Standard

Under 18 U.S.C. § 1345, a court may issue a preliminary injunction against ongoing violations of the wire fraud statute. *See United States v. William Savran & Assocs., Inc.*, 755 F. Supp. 1165, 1177–78 (E.D.N.Y. 1991). To obtain that remedy, the government must demonstrate probable cause to conclude that Defendants intended to engage in a "scheme to defraud." *See New York State Catholic Health Plan, Inc. v. Acad. O & P Assocs.*, 312 F.R.D. 278, 297 (E.D.N.Y. 2015). A scheme to defraud is "a plan to deprive a person of something of value by trick, deceit, chicane or overreaching." *Williams v. Affinion Grp., LLC*, 889 F.3d 116, 124 (2d Cir. 2018). The Defendants' intent can be shown by knowing participation in the fraud, or "reckless indifference to the truth." *See Catholic Health Plan*, 312 F.R.D. at 297.

Unlike in the usual preliminary injunction case, proof of irreparable harm is presumed under Section 1345 where the statutory conditions are met. *See Savran*, 755 F. Supp. at 1179. Concerns about fairness "do not drop entirely from the equation." *United States v. Narco Freedom, Inc.*, 95 F. Supp. 3d 747, 755 (S.D.N.Y. 2015). But where there is probable cause

that fraud is occurring, "the balance of hardships likely weighs in the Government's favor." *See id.*

Discussion

The government has introduced extensive, persuasive evidence that Defendants are aware of a substantial volume of fraudulent robocall traffic passing through their system. This evidence comes not only from the mountain of complaints made to the Defendants by other telecommunications entities, but also, as discussed below, from multiple individual fraud victims interviewed by government agents; call data from the Defendants' system obtained by the government; recordings of the substance of calls transmitted by the Defendants; and certain financial practices in which the Defendants engaged.

In brief, the fraud is alleged to work as follows: Defendants transmit millions of calls that "spoof" local area codes to mislead call recipients into believing that the incoming calls originated locally, given the greater likelihood that recipients will answer local calls. First Gerber Decl. ¶ 10. In fact, the calls usually originate abroad. *See id.*; First Ralston Decl. ¶¶ 35, 38; First Palumbo Decl. ¶ 17. To facilitate human contact with potential victims, Defendants sold direct-inward-dial ("DID") numbers and toll-free numbers (together, "call-back numbers") to robocallers, who could leave

those call-back numbers in messages on victims' voicemails. *See* First Gerber Decl. ¶¶ 16, 18; First Ralston Decl. ¶ 48.

Since 2017, Defendants have received no fewer than 100 separate notifications of fraudulent activity on their system. These notices came from state attorneys general; the common carrier AT&T; USTelecom, which is a trade association tasked with minimizing fraud in the robocalling industry; and other telecommunications providers. *See* First Ralston Decl. ¶¶ 30–40; *See* Dkt. No. 48, Second Gerber Decl. ¶¶ 4–10. The mechanism these entities use for filing and tracing complaints is called a "traceback." First Ralston Decl. ¶ 23.

For example, AT&T traced at least 20 fraudulent calls back to Defendants' system. *See id.* ¶¶ 39–40. AT&T notified Defendant Nicholas Palumbo that these calls "spoofed" numbers belonging to the United States Citizenship and Immigration Service ("USCIS") and Department of Homeland Security and were intended "to extort money from our customers." *Id.*

Between May 2019 and January 2020, defendant TollFreeDeals received 66 traceback notifications from USTelecom, which included notice of 42 calls purporting to originate with the SSA, IRS, or USCIS. *See* Second Ralston Decl. ¶ 4. Between August 2019 and December 2019, SIP Retail received 17 traceback notifications from USTelecom, which included notice of 12 calls from imposter SSA or USCIS officials. *See id.* ¶ 5.

Many of the complaints that came through these sources concerned "Company A."[6] Company A transmitted millions of calls through the Defendants' system and was the subject of a large volume of complaints, but Defendants continued to carry Company A's call traffic until the government filed this suit.[7] *See* Dkt. No. 49, Frankel Decl. Ex. 1, at 5. The government introduced evidence that multiple individual victims in the United States suffered significant fraud losses due to Defendants' business relationship with Company A.

For example, on June 5, 2019, one of those victims, L.U., received a call from a spoofed number that appeared to be the Federal Trade Commission's Consumer Response Center. Bracken Decl. ¶ 13. This call was transmitted through Defendants' system by Company A. *Id.* ¶ 14. The person who called him posed as an SSA official and told L.U. that his social security number was going to be suspended due to criminal activity if he did not provide his personal information. *Id.* ¶ 13. L.U. reported losing $2,200 as a result of this scam. *Id.*

[6] The government's declarations identified Company A by a pseudonym, and the names of all sixteen entities in Attachment A of the TRO are redacted because of the government's showing that naming them might affect ongoing investigations. Defendants know the identity of Company A. *See* Dkt. No. 54, Frankel Decl. filed under seal.

[7] For example, beginning on June 3, 2019, a USTelecom representative provided multiple warnings to Defendants that their system was being used to effectuate a Social Security scam. *See* Frankel Decl. ¶¶ 10–16. Defendants identified Company A as the client transmitting the calls. *See id.* Ex. 1, at 5. Defendants stated that they had reprimanded Company A but continued to do business with them. *See id.* ¶¶ 15–17.

On June 6, 2019, another call from Company A went to C.E., who had recently obtained U.S. citizenship and worked as an Uber driver. *Id.* ¶¶ 10–11. C.E. picked up a call transmitted by Defendants and was told he was speaking with an SSA agent named "George." *Id.* ¶ 10. The caller told C.E. that his social security number was being used in connection with criminal activity and connected C.E. with another person posing as a police officer. *Id.* The imposter police officer induced C.E. to give the fraudsters $700 to prevent his account from getting "seized." *Id.* ¶ 11.

Another foreign entity that sent calls through Defendants' network similarly defrauded an 84-year-old victim, J.K., who received a message from a person claiming to be from the U.S. Marshals Service. *Id.* ¶¶ 6–8. J.K. called the number left in the message and spoke with "George," who told J.K. that a warrant was out for his arrest because the police had found a car, which had been rented in his name, containing drugs, and J.K. needed to transfer money to prevent the police from seizing his bank account. *Id.* J.K. lost $9,800 to this scam. *Id.* ¶ 7. As with Company A, Defendants continued to do business with this company until the government filed suit.

The Palumbos acknowledge that prior to this suit, they never cut ties to any entity that they heard was associated with fraudulent call traffic, instead simply blocking the specific

number that placed the fraudulent call and passing the complaints along. *See* First Palumbo Decl. ¶¶ 25-26. Defendants knew or should have known, however, that these steps would be ineffective, given that the fraudulent calls were coming from a regularly rotating bank of spoofed numbers. *See* First Gerber Decl. ¶ 11; First Ralston Decl. ¶ 39.

On several occasions, the complaints passed back to Defendants contained a verbatim report of the contents of the fraudulent calls, rather than simply a victim's complaint about them. In one, for example, an automated voice claims the recipient's social security benefits are canceled until further notice, and that the recipient should "press 1" to speak with an SSA officer. *See* First Ralston Decl. ¶¶ 33-34.

Defendants have also recently received a series of civil investigatory demands from state attorneys general in Missouri and Indiana regarding investigations of illegal telemarketing calls routing through Defendants' system. *See* Second Gerber Decl. ¶¶ 4-10.

The number of complaints is, to be sure, relatively small in comparison to the enormous volume of calls that the Defendants transmit. But given that the telecom intermediary network is a "black box," as defense counsel acknowledged at

oral argument,[8] complaints are difficult to direct. Each "traceback" requires not only a call recipient to complain to their common carrier, but also the subsequent voluntary cooperation of every intermediary in the chain. First Ralston Decl. ¶ 23. And the individual robocalls complained about here are not bespoke. Indeed, the whole purpose of robocalling is to disseminate the same call content to large numbers of recipients simultaneously. It is therefore likely that each one of these complaints indicates the transmission of an exponentially higher number of fraudulent calls through the Defendants' network. *See* Frankel Decl. Ex. 1, at 3 ("A single complaint is representative of thousands of illegal calls (or more).").

At the very least, Defendants' failure to take meaningful action in response to these complaints demonstrates reckless indifference to the fraud they were enabling. Over time, it became increasingly clear that they knew or should have known the complaints evidenced a widespread pattern of fraudulent calls being transmitted over their network.

After the TRO entered by this Court on February 4, 2020 required Defendants to cease doing business with sixteen specified clients, it soon became apparent that Defendants'

[8] *See* Transcript of Mar. 3, 2020 Oral Argument ("Tr.") at 28:9; First Ralston Decl. ¶ 23 (describing tracebacks as a "labor intensive process"); *see also* First Dalrymple Decl. ¶ 8(b) (describing the multiple steps involved in tracing back a fraudulent call).

largest remaining client, Yodel, was also passing fraudulent call traffic through Defendants' network. *See* Dkt. No. 31-1. Evidence first arose in the form of new complaints about Yodel committing fraud. *See id.* Shortly thereafter, the government obtained and analyzed Defendants' "SIPNav" call data (call traffic data from the network traffic control platform that Defendants use), to which Defendants have also had access for years. *See* First Gerber Decl. ¶¶ 4–5. The government proceeded to sample the traffic evidenced in those records. A mere ten-minute sample of call data from January 24, 2020 shows Yodel routing over 6,000 robocalls through Defendants' network — including from at least eight numbers that have been publicly identified as originating government imposter calls. *See id.* ¶¶ 9–12. These identifications came courtesy of two companies, Nomorobo and YouMail, that make and manage "robo-blocking" software. *Id.* ¶ 12. Nearly all of these calls were "neighbor spoofed," meaning they appeared to originate from local phone numbers. *Id.* ¶ 10.[9]

[9] Sampling is an appropriate method here, given the millions of calls at issue. "The Supreme Court has observed that the decision of whether to award preliminary injunctive relief is often based on 'procedures that are less formal and evidence that is less complete than in a trial on the merits.'" *Mullins v. City of New York*, 626 F.3d 47, 51–52 (2d Cir. 2010) (quoting *Univ. of Tex. v. Camenisch*, 451 U.S. 390, 395 (1981)). Defendants' contention that the government should be required to review "a third" of the many hundreds of millions of calls traversing their network, *see* Tr. 48:15, is unreasonable at this stage.

These companies' findings reveal that the substance of the calls was consistent with the fraud under investigation in this case. Nomorobo's records relating to five of the Yodel numbers show they are part of an SSA scam in which an operator claims to be a "hearing administrator," calling on a "recorded line." *See id.* ¶ 12(a), (d), (e), (l), (m). YouMail's records relating to one of Defendants' numbers show that it, too, is involved in an SSA scam. *Id.* ¶ 12(k). Nomorobo's records also show that another number assigned to Defendants is being used for an SSA scam in which a "disability advisor" calls to discuss the recipient's "eligibility for Social Security disability benefits," *id.* ¶ 12(c); and yet another number has been used in an IRS imposter scam, *id.* ¶ 12(j). Also, complaints to the Michigan Attorney General's office regarding several fraudulent "SSA impersonation" calls were passed along to USTelecom, which in turn traced one of those calls back to Yodel. Dkt. No. 50, Halley Decl. ¶¶ 18–19.

Defendants' business of selling call-back (such as direct-inward-dial) numbers to clients is also a key element of the fraud. The call-back numbers provide a seamless way for the robocall victim-recipients to return calls, *see* Dkt. No. 55, Third Palumbo Decl. ¶ 8; in practice, this connects them with human fraudsters who, as in the case of J.K. above, seek to part them from their savings. In a two-month period in 2019,

Defendants received at least nine notifications from Teli Communications — a company that sells DID numbers to Defendants — that Defendants' clients were using these call-back numbers for nefarious purposes. *See* First Ralston Decl. ¶¶ 51–54. More recently, Defendants received a notification from Teli Communications that three call-back numbers that Defendants sold to Yodel were then used in IRS imposter scams. *See* Dkt. No. 31-1; *see also* Second Gerber Decl. ¶ 17.

Lastly, the government adduced evidence that at least some of Defendants' accounting and receivables practices are consistent with fraudulent activity. Despite maintaining their corporate banking relationship with J.P. Morgan Chase, Defendants went out of their way to set up another bank account at Wells Fargo to receive deposits from one client "who had difficulty with Chase bank." First Palumbo Decl. ¶ 46. The client in question then went on to make many large cash deposits, mostly in amounts slightly below $10,000. *See* Bracken Decl. ¶ 3 (noting that from May to September 2019, the Wells Fargo account received 19 cash deposits in at least five states across the United States totaling $130,250). Those deposits, in turn, were immediately transferred to Defendants' account at Chase. *See* Bracken Decl. ¶ 3. Defendant Nicholas Palumbo has now indicated, through counsel, that "he will never again accept any sort of deposits like that because now he knows better,"

Tr. 44:9–11; but these financial transactions provide further evidence that Defendants knew or should have known their clients were engaging in illicit conduct, or at a minimum, that Defendants were recklessly indifferent to such a risk.

For all these reasons, the Court is satisfied that the government has demonstrated probable cause to conclude that the defendants are engaged in a widespread patterns of telecommunications fraud, intended to deprive call recipients in the Eastern District of New York and elsewhere of money and property.

Remedy

The Court is conscious of the need to fashion a remedy that is proportional, as much as possible, to the specific harm here. *See e.g.*, *Sunward Elecs., Inc. v. McDonald*, 362 F.3d 17, 26 (2d Cir. 2004) ("By necessity, the scope of the injunction must be drawn by reference to the facts of the individual case, reflecting a careful balancing of the equities.") (quoting *Joseph Scott Co. v. Scott Swimming Pools, Inc.*, 764 F.2d 62, 67 (2d Cir.1985)). But I find that it is not possible to tailor the remedy more narrowly than the broad relief sought by the government — namely, preliminarily enjoining the Defendants from providing call termination services and from selling call-back numbers, including to Yodel. Whether by design or not, the telecommunications "intermediary" industry is set up perfectly

to allow fraudulent operators to rotate telephone numbers endlessly and blame other parties for the fraudulent call traffic they carry. Every day that the Defendants' actions in this vein continue, the public is at risk of harm in the form of additional high-dollar fraud losses. Section 1345 itself recognizes this urgency, requiring courts to proceed "as soon as practicable" to hear and determine the government's application for injunctive relief, and empowering courts not only to issue such relief, but also to "take such other action" as is warranted to prevent continuing and substantial injury. 18 U.S.C. § 1345(b).

In opposing the government's application for broad injunctive relief, Defendants focus much of their energy on their relationship with Yodel. They claim it would be unfair to foreclose their relationship with Yodel when that company comprises so much of their client base and the government has not pursued Yodel (which is now in bankruptcy) as part of this case. *See* Dkt. No. 43, Second Palumbo Decl. ¶¶ 2-3; Tr. 38:22–39:2.

But as laid out above, the government has introduced too much evidence here that Yodel is trafficking in fraudulent robocalling activity to acquiesce to this argument. This evidence includes not only the volume of complaints, but also, importantly, the government's analysis of the SIPNav data it

obtained, as well as the recorded evidence of the substance of the calls from Nomorobo. Indeed, the evidence of fraud is of substantially greater quality and quantity as to Yodel than it was to Defendants' dealings with Company A, which is covered by the TRO by the parties' mutual agreement. And given the astronomical volume of Yodel calls that the Defendants transmit, *see* First Gerber Decl. ¶ 14, the scope of the ongoing fraudulent activity is intolerably high even if the government has not shown that it constitutes the entirety of Yodel's call traffic to Defendants.[10]

Moreover, when balancing the equities on this particular question, I believe it appropriate to take judicial notice of another recent case involving Yodel. In a summary judgment order, another federal district court held that Yodel Technologies LLC violated the Telephone Consumer Protection Act ("TCPA") by engaging in "telemarketing" — *i.e.*, sales calls — without obtaining "consent from the called parties prior to initiating the calls." *Robert H. Braver v. Northstar Alarm Services LLC*, No. 17-cv-00383, 2019 WL 3208651, at *4 (W.D. Okla. July 16, 2019).[11]

[10] It is worth noting that Defendants have still not presented any affirmative evidence that Yodel transmits any "legitimate" call traffic, beyond the most conclusory assertions. *See* Dkt. No. 59, Fourth Palumbo Decl. ¶ 3.

[11] Defendants attempt to distinguish the Yodel entity that is the subject of the Western District of Oklahoma's findings of fraud, Yodel Technologies, LLC, from the entity with which Defendants do business, Yodel Technology

Obviously a TCPA violation is not evidence of fraud under Section 1343 or 1349. But if, as the government has persuasively demonstrated, there is simply no way to enjoin Defendants' fraudulent call traffic from Yodel apart from shutting down the relationship, then Defendants should be harder-pressed to complain about the *equities*, when even Yodel's purportedly non-fraudulent call traffic violates other federal law. *See, e.g.*, *United States v. Diapulse Corp. of America*, 457 F.2d 25, 29 (2d Cir. 1972) ("Nor can appellant complain that the injunction is impermissible because it will put him out of business. He can have no vested interest in a business activity found to be illegal." (internal quotation omitted)).[12]

Defendants raise a series of other arguments contending that a broad injunction would be premature at this point. First, they contend that before the Court grants the injunction, the government should have to obtain a wiretap and monitor calls on the Defendants' system. Tr. 50:9-14. But there is no legal

---

Services LLC. However, these Yodel entities are "under common ownership" and managed by the same CEO. *See* Dkt. No. 63-1, Wood Decl. ¶ 1. And as the government notes, Yodel Technologies lists Yodel Technology Services' assets and revenue in its Chapter 11 bankruptcy petition, *see* Dkt. No 60-2 at 11, 13-14, 26, and Yodel Technologies includes Defendant Ecommerce National LLC's accounts payable in its monthly operating report for January 2020, *see* Second Gerber Decl. ¶ 13. Accordingly, this Court does consider the Western District of Oklahoma's findings to be relevant — not dispositive, but relevant — to the question of whether the balance of equities favors permitting Defendants to do business with Yodel.

[12] Yodel has also been sued in other courts for violations of the TCPA. *See Keith Hobbs v. Randall-Reilly, LLC*, No. 4:19-cv-00009-CDL (M.D. Ga.); *Elcinda Person v. Lyft*, No. 19-cv-02914-TWT (N.D. Ga.).

support for the contention that Section 1345 requires such extraordinary preconditions, and there is already a significant amount of evidence regarding the volume and substance of the calls at issue.

Second, Defendants have belatedly offered to enact various "best practices," and urge the Court to grant them an opportunity to do so. *See* Dkt. No. 58 at 5-6. But actors such as the Defendants — who have demonstrated a willingness to engage in fraud even after myriad notifications — cannot be relied upon to change behavior simply because the government has now brought suit. Moreover, even as they promise to turn a new leaf, Defendants continue to contend that there is not much they can do about the fraudulent traffic on their network. *See, e.g.*, Dkt. No. 59, Fourth Palumbo Decl. ¶ 2 (stating that it is "impossible for a carrier like Ecommerce to know the precise data it carries").

Third, Defendants argue that the Court should hold an evidentiary hearing before granting the relief sought. But the grant of a preliminary injunction does not require an evidentiary hearing "when the disputed facts are amenable to complete resolution on a paper record," including affidavits. *See Charette v. Town of Oyster Bay*, 159 F.3d 749, 755 (2d Cir. 1998); *see also Mullins v. City of New York*, 626 F.3d 47, 52 (2d Cir. 2010) ("[H]earsay evidence may be considered by a district

court in determining whether to grant a preliminary injunction."). Indeed, another judge in this district recently entered a TRO on an *ex parte* basis in response to similar allegations, relying on the paper record. *See United States v. Kahen*, No. 20-cv-00474-BMC, Dkt. No. 7 (E.D.N.Y Jan 28, 2020).

Here, Defendants point to no specific facts in dispute that such a hearing would be valuable in resolving. On the contrary, the voluminous affidavit evidence, introduced to accompany several rounds of briefing and argument, has persuasively articulated probable cause to conclude that Defendants know their network is an instrumentality of a vast telecom fraud, and have knowingly facilitated that fraudulent traffic.

Including the Yodel evidence, the government has now submitted evidence demonstrating probable cause to conclude that Defendants' business is permeated with fraud. In light of this evidence, it would be untenable to require the government to continue to demonstrate ongoing fraudulent conduct on a client-by-client basis. The continued volume of fraud complaints to the Defendants even after the entry of the initial TRO supports these arguments.

Accordingly, the Court is persuaded that the only relief that will be effective in halting the fraudulent conduct here is a ban on the Defendants' continued provision of any call termination services for calls terminating in the United States,

and from providing call-back services. The government's motion for a preliminary injunction is GRANTED.

For the reasons set forth above, it is hereby ORDERED that Defendants, their agents, officers and employees, and all other persons and entities in active concert or participation with them, are enjoined from:

(1) providing, or causing others to provide, call termination services for calls terminating in the United States or carrying any VoIP calls terminating in the United States;

(2) providing direct-inward-dial or toll-free telephone services for calls originating in the United States, including providing toll-free phone numbers to other individuals or entities; and

(3) destroying, deleting, removing, or transferring any and all business, financial, accounting, and other records concerning Defendants' operations and the operations of any other corporate entity owned or controlled, in whole or in part, by Defendants.

IT IS FURTHER ORDERED that Somos, Inc., in its capacity as the entity designated by the Federal Communications Commission to administer the U.S. toll-free calling system and its database, is hereby ordered to temporarily suspend all toll-free numbers registered by or on behalf of any Defendant in this matter, until further order of this Court.

AND IT IS FURTHER ORDERED that any toll-free service provider that receives notice of this Order and has a contractual relationship with one of the Defendants in this matter to provide toll-free numbers, shall provide to Somos,

Inc. a list of all toll-free numbers provided to Defendant that are currently active.

SO ORDERED.

/s/ Eric Komitee
ERIC KOMITEE
United States District Judge

Dated: March 24, 2020
Brooklyn, New York